Contra-expertise beoordeling van de veiligheidsanalyse van de Nederlandse OV-Chipkaart door TNO[1]

Inleiding

In februari 2008 heeft TNO een openbaar rapport gepubliceerd waarin zij haar veiligheidsanalyse van de Nederlandse OV-chipkaart heeft samengevat. De analyse door TNO werd uitgevoerd in opdracht van Translink Systems (TLS) om een technische presentatie op een onlangs gehouden conferentie van de Chaos Computer Club (CCC) te beoordelen. In deze presentatie werd gesteld dat de kaarttechnologie en het algoritme van Mifare Classic waren gekraakt en in feite ongeschikt waren om de beveiliging van het OV-chipkaartsysteem van TLS op te baseren. Dit soort beweringen is schadelijk voor het publieke vertrouwen en zou, indien hardgemaakt, vervoersbedrijven nopen tot aanzienlijke en kostbare correctieve maatregelen en mogelijk veel ergernis en ongemak onder reizigers veroorzaken. Daarom zijn de bevindingen, conclusies en aanbevelingen van het TNO-rapport uiterst gevoelig, niet alleen vanuit een zakelijk oogpunt, maar evenzeer met het oog op de doelstellingen van de overheid en voor de acceptatie van het systeem door het publiek. Om deze reden heeft het Nederlandse ministerie voor Verkeer en Waterstaat een onafhankelijke contra-expertise (CE) laten uitvoeren om het TNO-rapport te beoordelen. Daarbij is de keuze voor het contra-expertisebureau (CEB) gevallen op de Information Security Group (ISG) van de de Royal Holloway University of London. Het project stond onder leiding van het ISG Smart Card Centre (SCC). De keuze viel op het CEB vanwege zijn onafhankelijke status en de deskundigheid op het gebied van informatiebeveiliging en smart cards die het projectteam in huis heeft, evenals uitgebreide ervaring op het totaalgebied van beveiliging van vervoerssystemen. Het Expertise Centrum (HEC) was verantwoordelijk voor de algehele facilitering van de opdracht en trad op als interface tussen het ministerie en het CEB.

De contra-expertise en de toegepaste methodiek

Het CEB was verzocht om een aantal specifieke vragen in zijn beoordeling aan de orde te stellen, te weten de volgende:

- Is er bij het opzetten/uitvoeren van het TNO-onderzoek gebruikgemaakt van een geschikte methodiek?
- Is het TNO-rapport volledig?
- Zijn de bevindingen, conclusies en aanbevelingen goed gefundeerd, juist en eenduidig?

Met bijzondere aandacht werden de aanbevelingen in het TNO-rapport bestudeerd om te zien of deze doeltreffend, realistisch, uitvoerbaar, volledig en toekomstbestendig zijn. De vraag aan het CEB was expliciet om de eigen onafhankelijke en professionele zienswijze te formuleren ten aanzien van de bevindingen, conclusies en aanbevelingen in het rapport. In essentie bestond de voor de contra-expertise gehanteerde methodiek uit het volgende:

- Een eerste beoordeling van de documenten die bij de contra-expertise betrokken worden.
- Interviews met TLS en TNO ter verduidelijking van de inhoud van de documenten en voor het uitwisselen van zienswijzen en ervaringen met betrekking tot de situatie rond de OV-Chipkaart.
- Gedetailleerde beoordelingen, inclusief de cryptografische aspecten, aanvalscenario's en methodiek.
- Systematische toetsing van het TNO-rapport aan de eisen van het ministerie.
- Formulering en rapportage van de zienswijzen en aanbevelingen van het CEB.

Tot de bij de contra-expertise betrokken documenten behoort het volledige TNO-rapport nr. 34642 (alsmede het openbaar gemaakte uittreksel). Ook werden recente publicaties over methodes om de OV-Chipkaart te kraken,

---

[1] Dit document bevat de vertaling van het in het Engels gepubliceerde rapport *Counter Expertise Review of the TNO Security Analysis of the Dutch OV-Chipkaart*, uitgebracht door Royal Holloway University of London (RHUL) aan het Ministerie VenW. In deze vertaling is de inhoud en strekking van het oorspronkelijke rapport zo nauwkeurig mogelijk benaderd, zodat het Nederlandse parlement en publiek hiervan zonder taalbarrière kennis kunnen nemen. Om echter discussie over mogelijke interpretatie- en nuanceverschillen te voorkomen, blijft het originele Engelse eindrapport van de RHUL het enige met formele status. Hoewel aan de vertaling zowel inhoudelijk als tijdens de totstandkoming uiterste zorg is besteed, aanvaardt het ministerie geen aansprakelijkheid voor eventuele fouten en onvolkomenheden, noch voor de gevolgen hiervan.

niet-gepubliceerd onderzoek[2] en overige relevante en publiekelijk toegankelijke informatie bij de beoordeling betrokken. Ter aanvulling daarop werd gebruikgemaakt van vertrouwelijke stukken afkomstig van TLS, waarin het algehele systeemontwerp plus bestaande detectie- en preventieve tegenmaatregelen om fraude en misbruik van beveiliging tegen te gaan, staan beschreven. TNO stelde ook een notitie ter beschikking over haar vervolgevaluatie voor TLS. Het resultaat van de contra-expertise is dit openbare rapport. Echter, alle gedetailleerde werkaantekeningen die zijn gebaseerd op gevoelige en vertrouwelijke informatie zijn ter ondersteuning van hun verdere onderzoek aan TLS en TNO ter beschikking gesteld. Het zij opgemerkt dat zowel TNO als TLS hun volledige medewerking hebben verleend aan deze contra-expertise en alle benodigde documentatie ter beschikking hebben gesteld, ervoor hebben gezorgd dat de juiste deskundigen beschikbaar waren om aan de vraaggesprekken deel te nemen en alle vragen die ter tafel kwamen, hebben beantwoord. Het CEB bedankt TLS en TNO voor hun medewerking bij deze beoordeling en ook de verschillende onderzoekers die ons deelgenoot hebben gemaakt van hun informatie, opmerkingen en suggesties.

De methodiek, de reikwijdte en de benadering van TNO

De algemene methodiek die TNO - zoals blijkt uit het gedetailleerde rapport - heeft gehanteerd, betreft ten eerste een onderzoek naar de Mifare kaarttechnologie (die aan de OV-chipkaart ten grondslag ligt) en de CCC-presentatie, alvorens de technische consequenties van de aanvallen in aanmerking te nemen, om deze vervolgens toe te passen op aanvalscenario's waar het vervoerssysteem in de praktijk mee te maken kan krijgen. Sommige delen van het rapport hadden betrekking op risicobeoordeling en het operationeel afhandelen van incidenten met behulp van detectie- en tegenmaatregelen in de back office. Ten slotte werden uit deze bevindingen conclusies getrokken en werden op basis daarvan aanbevelingen gedaan.

Het CEB is van oordeel dat de door TNO gehanteerde algemene methodiek geëigend was voor de opdracht, en dat het rapport - gezien de korte termijn waarbinnen zij de opdracht moest uitvoeren – blijk geeft van een opmerkelijke hoeveelheid professioneel en systematisch werk. Terecht werd het probleem benaderd vanuit het perspectief van het totale systeem, en werden praktijkscenario's, de beweegredenen en de uitvoering van criminele aanvallen, de beveiligingsmaatregelen op gegevens- en systeemniveau en het cryptografische algoritme van de kaart in aanmerking genomen. Het ware wellicht beter geweest als de methodiek van risicobeoordeling nauwer was gekoppeld aan de gevolgen die aanvallen hebben voor de reële financiële waarde, aangezien de financiële waarde kan wijzigen in de loop van de uitrol van het systeem (en in het algemeen in de loop van de tijd). Dit heeft op zijn beurt invloed op de aantrekkelijkheid van het systeem als doelwit van aanvallen en op het plannen van maatregelen ter beperking van de gevolgen van zulke aanvallen.

De scope van het TNO-rapport concentreert zich duidelijk op de gevolgen die de CCC-presentatie heeft op de vraag of men kan doorgaan met het gebruik van de op Mifare gebaseerde oplossingen met het CRYPTO1-algoritme en op de impact op het OV-Chipkaartsysteem. Het rapport laat uitdrukkelijk de Mifare Ultralight-kaart, die wordt gebruikt voor vervoersbewijzen voor eenmalig gebruik, buiten beschouwing. Uit vraaggesprekken bleek dat TNO er stellig van overtuigd was dat de Ultralight-kaart niet viel onder hun opdracht omdat voor deze kaart geen gebruik wordt gemaakt van CRYPTO1. Bovendien had TNO al eerder een onderzoek voor TLS uitgevoerd dat betrekking had op de Ultralight-kaart, waarin de problemen werden getypeerd en maatregelen werden voorgesteld om bepaalde misbruikscenario's tegen te gaan.

De benadering die TNO in meer algemene zin heeft toegepast, typeert het CEB als "evidence based", d.w.z. gestoeld op bewijzen, in tegenstelling tot de recente onderzoekspublicaties, die meer neigen naar een visionaire benadering. Hoewel in het TNO-rapport wordt beschreven in welke vormen aanvallen op het systeem en de algemene situatie zich in de toekomst zouden kunnen ontwikkelen, wordt in het rapport meer de nadruk gelegd op wat er op het moment van schrijven bekend, bewezen, gerechtvaardigd en gemeten was. Zo'n soort benadering is in veel gevallen terecht. Echter, gezien de zich aard van de situatie (snelle ontwikkelingen) wordt verwacht dat er een stroom aan vervolgpublicaties op gang zal komen waaruit blijkt dat de aanvallen sneller en beter zijn geworden. Hoewel het TNO-rapport dit erkent, zou het CEB ervoor gekozen hebben om bij het doen van aanbevelingen voor de toekomst aan deze factoren meer gewicht toe te kennen.

[2] Waaronder een concept-rapport van Nohl e.a. en vertrouwelijke informatie van de Radboud Universiteit van Nijmegen

Volledigheid van het TNO-rapport

Zoals reeds eerder vermeld, was de algemene methodiek die voor de totstandkoming van het rapport is gebruikt een geschikte; derhalve bevatte het rapport de te verwachten inhoudscategorieën. Het CEB was specifiek gevraagd om commentaar te geven op de vraag of TNO alle niveaus van het systeem evenredig veel aandacht had gegeven:

- Level 0 = De kaart
- Level 1 = Terminal-/leesapparatuur
- Level 2 = treinstations, systemen op busstations/remises
- Level 3 = systemen van de openbaar vervoer bedrijven (OVB's)
- Level 4 = Systemen voor centrale verwerking

Het TNO-rapport bevatte een gedetailleerde behandeling van level 0 en level 4 en een minder gedetailleerde, maar niettemin toereikende behandeling van level 1. Level 2 en level 3 werden buiten beschouwing gelaten. In vraaggesprekken met zowel TLS als TNO werd uitgelegd dat de ontbrekende levels momenteel geen functionele rol spelen die voor de beveiliging en voor de opsporing van fraude van belang is. Wel werd opgemerkt dat de OVB's een duplicaat van de loggegevens van de reistransacties ontvangen. Deze gegevens worden momenteel slechts gebruikt als extra controle van het financiële verrekeningsproces. Op grond van deze duplicaten van transactieloggegevens en de gedetailleerde kennis die de OVB's hebben van hun infrastructuur zou wellicht kunnen worden overwogen om OVB's te betrekken bij het identificeren van de locaties (bijv. bepaalde stations) waar fraude plaatsvindt.

De beschrijving van het Mifare CRYPTO1-algoritme was beknopt, aangezien TNO zich hiervoor uitsluitend had gebaseerd op publiek toegankelijke documentatie, en aan TNO door NXP geen verdere bijzonderheden waren verstrekt. Naar het oordeel van het CEB hoeft dit niet in belangrijke mate af te doen aan de waarde van het TNO-rapport, aangezien deskundigen reeds geruime tijd op de hoogte zijn van de meest voor de hand liggende en fundamentele beperkingen van CRYPTO1:

- Dat het algoritme een zeer korte (48-bit-)sleutel gebruikt.
- Dat de beveiliging van de kaart in sterke mate afhangt van de geheimhouding van het algoritme.

TNO en het CEB zijn beide van mening dat afhankelijkheid van de geheimhouding van het algoritme volstrekt tegengesteld is aan de aanbevolen beste praktijk ten aanzien van cryptografische systemen. Door deskundigen wordt dit laatdunkend 'security by obscurity' genoemd en dat is tevens een van de redenen waarom CRYPTO1 zo'n geliefd doelwit is voor aanvallen. Dankzij de meest recente publicaties is er in het publieke domein al een aanzienlijke hoeveelheid informatie beschikbaar over het algoritme en naar verwachting zal deze informatie alleen maar toenemen, waardoor aanvullende informatie van NXP niet van wezenlijk belang lijkt te zijn. Indien echter TNO alle informatie over het algoritme was verstrekt, dan zou dit in de evidence-based benadering van TNO van pas zijn gekomen, en zou er minder noodzaak tot speculatie over de potentiële structurele zwakke plekken en daarmee verband houdende aanvalscenario's zijn geweest.

De bespreking van de CCC-presentatie was toereikend en dit leidde tot meer gedetailleerde informatie over de technische en beveiligingstechnische gevolgen die op haar beurt leidde tot allerlei aanvalsstrategieën. Dit hoofdstuk bood een aanzienlijke hoeveelheid informatie waarbij vele technieken de revue passeerden. De informatie was niet geheel compleet, want ten minste één aanvalsstrategie werd weggelaten en ook ontbraken sommige technieken die aanvallen met beperkte hardwaremiddelen eenvoudiger zouden kunnen maken. Uit de vraaggesprekken kwam naar voren dat TNO vervolgens in het kader van een vervolg onderzoek voor TLS een verdere analyse heeft gemaakt van nog enkele aanvalsstrategieën/technieken; de resulterende notitie is met het CEB gedeeld. Het hoofdstuk over misbruik, waarin aanvalstechnieken werden toegepast op praktijkscenario's, was zeer gedetailleerd, hoewel zonder de ontbrekende aanvalscenario's/technieken. Ook aan de orde kwamen het criminele gebruik van verschillende soorten apparatuur en gekloonde kaarten, waarbij één praktijkvoorbeeld van een zakelijke afweging werd gepresenteerd en besproken. Ook kwamen de gevolgen van het kraken van kaarten voor de verschillende belanghebbenden aan bod, waarbij ook een korte paragraaf werd gewijd aan de privacy van de klanten.

Er was aanzienlijk veel aandacht voor operationele afhandeling van beveiligings- en fraude-incidenten, die een bestudering van de vele bestaande validaties en rapportageverwerkingsregels die door de back-endsystemen van TLS worden uitgevoerd, noodzakelijk maakte. Eveneens werden in de beschouwing betrokken de beschikbare mechanismen voor het onbruikbaar maken van ongeldige of verdachte kaarten. Hoewel dit hoofdstuk zeer informatief is, kan het niet als geheel volledig worden beschouwd, omdat niet precies is aangegeven hoeveel tijd benodigd is om op afzonderlijke gebeurtenissen te reageren. Dergelijke informatie is nodig om met nauwkeurigheid te kunnen bepalen hoe lang gekloonde kaarten of kaarten met frauduleuze wijzigingen kunnen worden gebruikt. Het was op basis van vraaggesprekken met TNO en TLS mogelijk om de standaardresponstijd die in het TNO-rapport wordt vermeld, te valideren, hoewel deze was gebaseerd op de huidige lichtbelaste situatie waarin sprake was van slechts een klein aantal af te handelen incidenten. TNO en het CEB zijn het er echter over eens dat er ruimte is voor TLS om de personeelsinzet, de geautomatiseerde systemen en de responssnelheid aan te passen mocht het aantal incidenten significant toenemen. Momenteel echter zijn er te weinig statistische gegevens beschikbaar om deze toename te kunnen helpen voorspellen of typeren.

Zoals eerder vermeld wordt de risicobeoordeling niet als geheel volledig beschouwd, omdat de effecten niet rechtstreeks werden gekoppeld aan financiële waarde en de frequentie van geslaagde aanvallen. Daarnaast werden het type en de technische/financiële mogelijkheden van de aanvaller(s) niet uitdrukkelijk vermeld. Bij vraaggesprekken met TNO werd bevestigd dat de waarschijnlijkheid van incidenten meer was gebaseerd op criminele aanvallen dan op proof-of-concept-aanvallen door onderzoekers. Om de gevolgen van risico's te beperken werd een aantal zorgvuldig beredeneerde verbeteringen van de huidige systeemoplossing voorgesteld, hoewel de uitvoerbaarheid en doeltreffendheid van die maatregelen nog niet helemaal zijn bewezen.

Correspondentie tussen bevindingen en conclusies/aanbevelingen

In het algemeen zijn de gedetailleerde vraagstukken en aanvallen in het kader van het TNO-rapport op een logische en goed gefundeerde wijze onderzocht. Het gebruik van de bevindingen bij de totstandkoming van de conclusies en aanbevelingen werd niet enkel gebaseerd op beschikbaar feitenmateriaal, maar berustte mede op veronderstellingen vanuit eerdere ervaringen van TNO.

Er is sprake van een heldere conclusie waarbij één boodschap als rode draad door het rapport heenloopt: de Mifare Classic-kaart zal moeten worden vervangen. Er worden enkele suggesties op hoog aggregatieniveau gedaan ten aanzien van de keuze van een opvolger waarnaartoe kan worden gemigreerd, hoewel de aanbevelingen geen rechtstreeks verband leggen met internationale normen, beveiligingsbeoordeling of beste praktijken op het gebied van cryptografie.

Hoewel de essentie van de conclusie juist was, werden enkele veronderstellingen ten aanzien van technologische barrières tegen aanvallen ondermijnd door het eerder genoemde ontbreken van aanvalscenario's en –technieken. Deze veronderstellingen zijn cruciaal voor het inschatten van de snelheid waarmee een aanval kan worden uitgevoerd en de daarvoor benodigde investering en kennis. Er werd geen duidelijk verband gelegd tussen de aantrekkelijkheid van het systeem als doelwit voor een aanval en de waarde van aanvallen of de implementatiefases van het systeem. Gekoppeld aan de technische veronderstellingen gaf dit de aanbevelingen voor de tijdsplanning een grote marge. Deze marge wordt nog groter als men bedenkt dat de plannen afhankelijk zijn van de uitvoering van aanvullende (thans onbewezen) tegenmaatregelen. Gezien de ruime marge is het onwaarschijnlijk dat de aanbeveling van TNO ten aanzien van de mijlpaal voor migratiegereedheid een zeer nauwkeurige schatting is voor de afronding van de complexe opeenvolging van werkzaamheden.

De conclusies en aanbevelingen zeggen weinig over hoe de publieke opinie, reputatieschade voor bedrijven en wijzigingen in het gedrag van de klanten van invloed kunnen zijn op de planning van de migratie. Verder lijken er geen expliciete aanbevelingen te worden gedaan in de richting van het toekomstbestendig maken van het gemigreerde systeem.

Beoordeling van het TNO-rapport: De conclusies en aanbevelingen van het CEB

De CEB is met TNO van oordeel dat de Mifare Classic 4k, die in de OV-Chipkaart wordt gebruikt, zal moeten worden vervangen. Het CEB zou een stap verder willen gaan en aanbevelen dat elke vervanging zou moeten worden gebaseerd op een algoritme dat rigoureus is geëvalueerd door de gemeenschap van cryptografiedeskundigen, waarvan de beveiliging niet staat of valt met de geheimhouding van het algoritme en dat gebruikmaakt van een sleutellengte conform de cryptografische aanbevelingen [2]. Aan deze aanbeveling ligt de overtuiging van het CEB ten grondslag dat er reverse-engineering van CRYPTO1 heeft plaatsgevonden en wel in die mate dat het niet langer als geheim kan worden beschouwd. Er doen al geruime tijd verhalen de ronde dat er ongelicentieerde Mifare-producten op de markt verkrijgbaar zijn die gebruikmaken van het CRYPTO 1-algoritme. Het is daarom zeer waarschijnlijk dat deze reverse-engineering al had plaatsgevonden voordat de CCC-presentatie werd gehouden. Echter, zelfs al zou dit niet het geval zijn, dan nog doen de CCC-presentatie en daaropvolgende publicaties vermoeden dat de volledige openbaarmaking van alle laatste details van het algoritme niet lang op zich zal laten wachten. Men moet er niet van uitgaan dat deze openbaarmaking alleen te verwachten valt uit de groep achter de CCC-presentatie, want er zijn andere expertteams die deze laatste details kunnen deduceren nu ze door de grote aandacht van de media in de verleiding worden gebracht om deze taak op zich te nemen. Het CEB onderschrijft het TNO-rapport waar wordt gesteld dat CRYPTO1, zodra het volledig openbaar is gemaakt, zich leent voor apparatuur waarmee geheime sleutels kunnen worden achterhaald.

Het CEB meent dat apparatuur waarmee sleutels snel kunnen worden gekraakt verhoudingsgewijs goedkoop en eenvoudig verkrijgbaar is, maar sluit niet uit dat er alternatieve technieken zijn (bijvoorbeeld vooraf-berekening) die nog goedkoper, sneller en eenvoudiger zijn. Dankzij het voordeel van publicaties die ten tijde van het TNO-rapport nog niet beschikbaar waren, houdt het CEB er verder rekening mee dat de zwakke plekken in het algoritme zullen worden benut voor het kraken van sleutels met apparatuur die aanzienlijk minder specialistisch en kostbaar is. Het is inderdaad een bekend gegeven dat de veiligheid van leverancier-eigen bitstroomencryptie "uiteenvalt" zodra deze wordt onderworpen aan een nauwgezet onderzoek door cryptografische deskundigen. Het TNO-onderzoek ging uit van een als privé-initiatief ontwikkelde aanvalsinstallatie van een individuele groep, met overeenkomstige implicaties voor de vereiste inspanning, moeilijkheidsgraad en tijd. Echter, gezien de grote media-aandacht voor het OV-Chipkaartsysteem is het heel wel mogelijk dat er teams worden gevormd waarin deskundigen vanuit verschillende expertisegebieden samenwerken, waardoor een snelle ontwikkeling en geoptimaliseerde aanvallen mogelijk worden.

Het CEB deelt de zienswijze van TNO dat een aanvaller, zodra de geheime sleutels van een kaart zijn achterhaald, de inhoud van de kaart in een elektronische kaartemulator of in een ander type kaart (een kloonplatform) kan wijzigen of deze kan kopiëren. Het achterhalen van de geheime sleutels verschaft de aanvaller maximale gelegenheid en flexibiliteit, hoewel het in sommige gevallen mogelijk kan blijken om de inhoud van een uitgegeven kaart te wijzigen zonder kennis te hebben van de sleutels. Evenmin als TNO is het CEB erin geslaagd om een scenario te vinden waarbij kennis van CRYPTO1 ertoe zou kunnen leiden dat de moedersleutel van een systeem wordt achterhaald.

Het CEB onderschrijft niet de publieke stelling van TNO dat een gekloonde kaart er noodzakelijkerwijs anders uitziet dan een authentieke OV-Chipkaart. Het CEB heeft een aantal authentieke voorbeelden van ontwerpen voor de OV-Chipkaart gezien en van sommige daarvan menen wij dat deze betrekkelijk eenvoudig moeten kunnen worden gereproduceerd. Tijdens de vraaggesprekken met TNO werd ons te kennen gegeven dat men met gekloonde kaarten in deze context doelde op de hardware-emulators in de vorm van printplaatjes in kaartformaat, aangezien men van mening was dat echte kaarten met minder waarschijnlijkheid zouden voorkomen. Hoewel deze hardware-emulators op de korte termijn zouden kunnen worden gebruikt, meent het CEB dat men erop voorbereid moet zijn dat er geschikte chips voor smart cards op de markt zullen komen. Deze chips zouden aanvallers vervolgens kunnen verwerken in een kaart die eruitziet als een echte OV-Chipkaart. Het CEB

2 Zie http://www.keylength.com/en/3/ voor cryptografische aanbevelingen voor sleutellengte van verschillende deskundige organisaties

begrijpt dat sommige van de voorgestelde maatregelen om aanvallen tegen te gaan ertoe kunnen leiden dat er grotere nadruk komt te liggen op fysieke kaartcontrole door controleurs, in welk geval de fysieke verschijningsvorm van de kaart van groter belang is. Er schijnen momenteel veel kaartontwerpen te zijn (en dat worden er in de toekomst nog meer). Daardoor kan het voor een kaartcontroleur moeilijk worden om op het oog het verschil te zien tussen een echte en een vervalste kaart. Aanbevolen wordt derhalve dat toekomstige OV-Chipkaarten (afgezien van het gebruikte cryptografisch algoritme) in elk geval één gezamenlijk en herkenbaar antifraudekenmerk dragen, bijvoorbeeld een lasergravure of een hologram.

TNO concludeerde dat de scenario's voor systeemmisbruik beperkte gevolgen hebben voor de kaarthouders. Het CEB is het er weliswaar mee eens dat de financiële schade beperkt zou blijven, maar onder gevolgen kan ook de vrees worden begrepen die het gevolg is van het bekend worden van proof-of-concept-aanvallen waarbij nog geen sprake is van criminele activiteiten. Een criminele aanval kan zich richten op het kaartsaldo of opwaarderingen daarvan, en hoewel de kaarthouder deze schade vergoed zou moeten krijgen, zal zo'n ervaring wederom een bron van narigheid en ergernis vormen. Om dit in het juiste perspectief te plaatsen moet echter wel gesteld worden dat burgers veel meer kans lopen slachtoffer te worden van fraude en misbruik bij gebruikmaking van algemene diensten via het internet of de telefoon.

Het CEB kan zich wel vinden in de conclusie van TNO dat gegevensprivacy geen hoofdprobleem vormt voor de OV-Chipkaart, omdat de chip zelf momenteel alleen de geboortedatum en enige reisgegevens bevat, waardoor het als bron voor persoonlijke gegevens weinig te bieden heeft vergeleken met bijvoorbeeld phishing.[3] Echter, het CEB erkent dat privacy een zaak van persoonlijke opvatting is. Elke bedreiging die wordt ervaren en waaraan niet op behoorlijke wijze aandacht wordt geschonken, zou kunnen leiden tot nog verder verlies van vertrouwen.

Huidige en toekomstige aanvallen kunnen ervoor zorgen dat het publiek het vertrouwen in de OV-Chipkaart en zelfs in andere kaartsystemen kwijtraakt, ongeacht de onderliggende technologieën. Ook kan het bij sommige klanten leiden tot negatieve gedragswijzigingen terwijl de media-aandacht voor proof-of-concept-aanvallen aan kan zetten tot pogingen tot andere vormen van fraude. Bovendien kunnen sommige kaarthouders, als de aanvalstechnieken eenvoudig genoeg zijn geworden, in de verleiding komen zelf als amateur-aanvaller aan de slag te gaan om hun persoonlijke reiskosten te drukken.

TNO heeft weliswaar oog voor de financiële schade die een vervoerbedrijf zou kunnen ondervinden, maar heeft minder aandacht voor de reputatie van het bedrijf en voor secundaire effecten. De impact op de vervoersbedrijven wordt niet alleen afgemeten aan de financiële schade als gevolg van fraude, maar aan een reeks factoren, waaronder het effect op de bedrijfsreputatie. Helaas zal er, zodra er proof-of-concept-aanvallen gepubliceerd worden, waarschijnlijk sprake zijn van aanzienlijke gevolgen die deels losstaan van de hoeveelheid criminele aanvallen. Op basis van ervaring met een andere situatie waarin sprake was van klonen, is bekend dat dit kan leiden tot een stortvloed aan klachten, claims en informatievragen van klanten waardoor er een omvangrijk beroep wordt gedaan op de klantenservice en technisch-onderzoekers. Het is daarom van belang dat er rekening mee wordt gehouden dat een besluit over een technologische migratie evenzeer kan worden beïnvloed door reputatieschade die een bedrijf heeft ondervonden en door de kosten van extra inzet van middelen, als door de financiële gevolgen van de aanvallen zelf.

TNO heeft in haar aanbevelingen gesteld dat "er geen acute noodzaak voor migratie is", maar vervolgens wel de noodzaak benadrukt om "migratie gereedheid" te bereiken. Bij de eerste beoordeling van het openbare TNO-rapport vatte het CEB deze beweringen op als verraadden zij een ietwat lichtvaardige opstelling ten opzichte van migratie. Echter, uit de vraaggesprekken kwam naar voren dat TNO deze indruk niet had willen wekken. Duidelijkheidshalve wordt de uitleg die tijdens het vraaggesprek door TNO werd gegeven, hier weergegeven. De redenering van TNO die achter de eerste bewering ligt, is dat er momenteel geen enkel bewijs is voor zulke aanvallen op het TLS-systeem. Daarbij zijn er slechts twee lokale vervoerssystemen waarbij een chipkaart kan worden gebruikt voor laaggeprijsde ritten en beperkte kaartsaldi, waardoor het systeem

3 Phishing is een wijdverbreide criminele techniek waarbij gebruikers via e-mail persoonlijke en financiële informatie wordt ontfutseld.

niet een erg aantrekkelijk (zakelijk) doelwit vormt voor crimineel misbruik. Ook wordt ervan uitgegaan dat de correctieve maatregelen en tegenmaatregelen die door TNO worden voorgesteld, uitvoerbaar blijken en zijn doorgevoerd binnen het systeem. Het "migratiegereed zijn" werd uitgelegd als de fase waarin alle OVB's de nieuwe lees-/terminalapparatuur op alle treinstations en in alle bussen in gebruik hebben genomen, waardoor de daaropvolgende migratie hoofdzakelijk zou bestaan uit de invoering van een nieuwe kaart.

Het CEB sluit zich aan bij de visie dat het systeem betrekkelijk oninteressant is voor criminelen omdat het systeem alleen geschikt is voor laaggeprijsde ritten en lage kaartsaldi (hoewel men meer openbare proof-of-concept-demonstraties zou verwachten). In dat geval zou het bestaande brede scala aan backoffice-detectie en responsmechanismen de bedreiging op de korte termijn kunnen compenseren. Deze compensatie kan echter wegvallen wanneer het systeem landelijk wordt ingevoerd, omdat het dan om grotere bedragen gaat voor zowel de ritprijzen als de kaartsaldi en het systeem dus een veel interessanter doelwit voor aanvallen wordt. De tegenmaatregelen die TNO heeft voorgesteld zouden bescherming kunnen bieden tegen sommige aanvalscenario's, maar de uitvoerbaarheid van die maatregelen is nog onvoldoende bewezen. Dit moet nu met urgentie worden onderzocht.

Migratiegereedheid volgens de definitie van TNO is een zeer belangrijke fase, omdat PTO's op dat moment een aantal cruciale planningsfases moeten hebben doorlopen en aanzienlijk hebben geïnvesteerd in apparatuur en personeel om de nieuwe infrastructuur te kunnen uitrollen. Op het moment beschikt het CEB niet over statistische gegevens of referenties waarmee op betrouwbare wijze de juistheid van de inschatting van TNO, dat het zo'n twee jaar zal duren voordat het stadium van migratiegereedheid is bereikt, kan worden geverifieerd of bestreden. Om dit nader te kunnen onderzoeken zijn er gedetailleerde migratieplannen nodig aan de hand waarvan mede kan worden bepaald of er voor het ingaan van zo'n migratie sprake moet zijn van een enkele doorslaggevende gebeurtenis ('trigger event') of dat er bij voorkeur sprake moet zijn van een stapsgewijze invoering naarmate er zich op bepaalde gebieden meer beveiligingsproblemen voordoen. In het TNO-rapport wordt de suggestie gewekt dat de technologie verder moet worden ontwikkeld voordat snelle en goedkope aanvalsmethoden binnen handbereik van criminelen komen. Deze factor kan hebben meegespeeld om tot de inschatting van de twee jaar te komen. Echter, recent onderzoek lijkt deze zienswijze te weerspreken.

Het CEB raadt met klem een eerdere, tussentijdse mijlpaal aan, de zogeheten **Mijlpaal voor migratieplanning**, die vastgezet is op januari 2009 om samen te vallen met de geplande voltooiing van de landelijke uitrol van het huidige systeem. Zo wordt gewaarborgd dat er vanaf de start van de landelijke invoering sprake is van gereedheid om te migreren naar een hoger niveau van kaartveiligheid. In dit migratieplan zouden alle noodzakelijke activiteiten, betrokken partijen, budgetten en technologie moeten staan beschreven. Van open communicatie over de vooruitgang in de richting van de mijlpaal kan eventueel een afschrikkende werking uitgaan naar aanvallers. Daarnaast zou een onafhankelijke beoordeling van de conceptversies van het plan het vertrouwen in het slagen van migratie versterken. Voordat de mijlpaal bereikt is, moet er veel werk worden verzet, zoals het uitvoeren van een gestructureerde risicoanalyse, het identificeren van de nieuwe kaarttechnologie, het definiëren van verbeteringen van de infrastructuur, het selecteren van leveranciers, het verkrijgen van budgetten en alle overige reguliere en logistieke werkzaamheden die komen kijken bij project- en planning. Met het nemen van deze maatregelen, die vergelijkbaar zijn met de maatregelen die door TNO zijn voorgesteld, is er nog geen sprake van fysieke invoering. De uiteindelijke beslissing om met de migratie van start te gaan zou op een later moment genomen kunnen worden, gebaseerd op afgesproken procesvoering en doorslaggevende factoren ('triggers') - zoals het gemeten fraudeniveau[4] - die zijn gedefinieerd in het migratieplan.

Het CEB erkent dat een migratieplan idealiter beschikbaar zou moeten zijn vóór de mijlpaal voor de migratieplanning, maar het werkprogramma zou zeer moeilijk zijn en de vervoersbedrijven zouden de tijd moeten nemen om advies in te winnen onder internationale deskundigen, zoals een aantal onderzoekers reeds met klem heeft geadviseerd. Het laatste waar nu behoefte aan is, is dat er met betrekking tot de migratietechnologie een overhaaste besluitvorming plaatsvindt op basis van onjuiste of onvolledige informatie, gevolgd door een invoering die slecht is gepland en slecht wordt uitgevoerd.

4 Toegeschreven aan het probleem van de kaartbeveiliging.

De tijd tot aan de voorgestelde mijlpaal voor de migratieplanning biedt ook een redelijke termijn waarbinnen de eerste statistische gegevens met betrekking tot de aanvallen die in werkelijkheid plaatsvinden kunnen worden verzameld, en de doeltreffendheid en uitvoerbaarheid van de tegenmaatregelen uit het TNO-rapport beoordeeld. Tegenmaatregelen eerder invoeren kan worden overwogen als de voordelen de kosten en inspanningen daarvan rechtvaardigen in vergelijking met het wachten op de oplossing door kaartmigratie.

Het TNO-rapport bevatte geen voorstellen waarvoor een ‘toekomstbestendigheidsgarantie’ kon worden gegeven. Daarom wil het CEB, uitgaande van eigen ervaringen, gaarne aanvullende suggesties doen welke bij de migratieplanning in overweging kunnen worden genomen. De migratie naar een andere kaart/een ander algoritme moet niet worden beschouwd als een eenmalige gebeurtenis, maar als een kans om het systeem zodanig in te richten dat deze kan beantwoorden aan welke toekomstige migratiebehoeften dan ook. Wij raden daarom aan om op korte termijn modularisatie van de beveiligingsoplossing voor de kaart en de kaartlezer te overwegen, zodat meerdere kaarten/algoritmes zouden kunnen worden ondersteund. Dit zorgt er niet alleen voor dat het systeem toekomstbestendiger wordt, maar ook dat een gefaseerde migratie tussen verschillende kaarttypes wordt ondersteund. Een voordeel van gefaseerde migratie is dat bestaande kaarten tot aan de afloop van hun normale gebruiksduur kunnen worden gebruikt voordat ze worden vervangen, waardoor de klanten kosten en ongerief worden bespaard.

Voor de verdere toekomst zou de modulaire benadering verder kunnen worden uitgebreid, zoals ook is gebeurd in de mobiele communicatie. De interface naar het authenticatiealgoritme van de smart card en de algemene functionele vereisten zijn gedefinieerd en gepubliceerd in internationale normen. Voor het authenticatiealgoritme zelf bestaat echter geen standaard[5]. Dit stelt bedrijven in staat om voor gedifferentieerde beveiligingsoplossingen te kiezen en biedt tegelijkertijd een kader dat de gefaseerde migratie van algoritmes ondersteunt. In het geval van mobiele telefonie van de derde generatie (3G), heeft een internationale groep beveiligingsdeskundigen een open en vrij beschikbaar voorbeeldalgoritme gepubliceerd, dat nu in brede kring aanvaard is.

Welke methodes en expertise ook worden ingezet om te zorgen dat er voor het algoritme voor de OV-Chipkaart een geschikte vervanger wordt gekozen, het is minstens zo belangrijk om het algoritme op een veilige en aanvalbestendige wijze in te voeren. Daarom moet worden overwogen om de implementatie van het algoritme in de slimme kaart en in de systeeminfrastructuur te onderwerpen aan een onafhankelijke beoordeling[6].

Een andere algemene manier waarmee de toekomstbestendigheid van een willekeurig systeem wordt versterkt is door bijzondere aandacht te schenken aan risicomodellering. Eigenlijk wil het CEB met de grootst mogelijke nadruk erop wijzen dat er bij het ontwerpen, invoeren, exploiteren en verbeteren van cruciale systemen van deze aard zeer strenge risicobeoordelingsmethodieken moeten worden toegepast. In het geval van het OV-Chipkaartsysteem zouden alle momenteel gebruikte kaarttypes aan deze risicobeoordeling moeten worden onderworpen, inclusief de Mifare Ultralight.

Ter afsluiting wil het CEB de huidige problemen in perspectief zetten door te onderstrepen dat smart card systemen in andere landen en bedrijfstakken succesvol zijn en populair onder klanten vanwege de geboden snelheid, flexibiliteit en gemak. Organisaties die met kaartverkoop te maken hebben, zien hierdoor niet zelden kans de kosten van de productie en verkoop van kaartjes te verminderen en (wellicht voor het eerst) gevallen van niet-technische fraude, die mogelijk is met papieren kaartjes of kaartjes met magnetische strips, op te sporen en in te dammen. Wil men met de invoering van een op de smart card gebaseerd vervoerssysteem deze voordelen benutten, dan gelden als belangrijkste uitdaging de implementatie van het systeem, de zakelijk-financiële infrastructuur en het inrichten van daarmee verbonden operationele processen. Ook van vitaal belang is de beleving van de klant, omdat een vervoerssysteem nu eenmaal is bedoeld voor een comfortabele en snelle doorstroom van reizigers. Ook al vormen de smart card en de daaraan gerelateerde lezermodules cruciale elementen in de systeemoplossing, zij vormen slechts een betrekkelijk klein deel van de uitdaging van de inrichting van de infrastructuur; derhalve moeten zij als onderdeel van een gefaseerd migratieproces eenvoudig te vervangen zijn.

5 Het zij opgemerkt dat algoritmes voor gegevensversleuteling zijn gestandaardiseerd om apparatuur onderling te kunnen laten samenwerken en ten behoeve van roaming.

6 Bij voorkeur conform internationale normen